ASSESSMENT OF A STRATEGIC PARTNERSHIP BETWEEN THE U.S. DEPARTMENT OF HOMELAND SECURITY SCIENCE AND TECHNOLOGY DIRECTORATE AND THE U.S. ARMY DEVELOPMENTAL TEST COMMAND

Research Report

Dennis A. Teefy

May 2011

PUBLISHED BY
Dennis A. Teefy
PROJECT ADVISER
Michael Zwibel
Defense Acquisition University
Senior Service College Fellow
5027 Black Hawk Rd
Aberdeen Proving Ground, MD 21010

Report Documentation Page

Form Approved
OMB No. 0704-0188

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
MAY 2011		**00-00-2011 to 00-00-2011**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Assessment Of A Strategic Partnership Between The U.S. Department Of Homeland Security Science And Technology Directorate And The U.S. Army Developmental Test Command	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Defense Acquisition University,Senior Service College Fellow,5027 Black Hawk Rd,Aberdeen Proving Ground,MD,21010**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**48**	

PAGE LEFT BLANK INTENTIONALLY

ASSESSMENT OF A STRATEGIC PARTNERSHIP BETWEEN THE U.S. DEPARTMENT OF HOMELAND SECURITY SCIENCE AND TECHNOLOGY DIRECTORATE AND THE U.S. ARMY DEVELOPMENTAL TEST COMMAND

Research Report

Dennis A. Teefy

May 2011

PROJECT ADVISER
Michael Zwibel

Defense Acquisition University
Senior Service College Fellow
5027 Black Hawk Rd
Aberdeen Proving Ground, MD 21010

DISCLAIMER

The contents of this paper are the sole result of the research performed by the author. The results are the opinions solely of the author and do not reflect the opinions of the TACOM Life Cycle Management Command, the Defense Acquisition University, or the U.S. Army.

TABLE OF CONTENTS

PAGE LEFT BLANK INTENTIONALLY

ABSTRACT

There are thousands of books, articles, and theories based on organizational management and growth. This research paper takes two of the hundreds of documented planning techniques to identify opportunities and issues facing a partnership between the U.S. Army Developmental Test Command (DTC) and the U.S. Department of Homeland Security (DHS) Science and Technology (S&T) Directorate.

On the surface, the potential for cooperation and teaming seems straightforward and logical. DHS S&T has technology testing needs to support its acquisition programs, and DTC has established test facilities and workforce already meeting similar needs for the U.S. Army. Upon further inspection, the issue requires the evaluation of two problems: (1) Is it possible? (2) How to make it happen. This research paper focuses solely on the first problem. To answer if it is possible, this research paper uses two approaches. First, a comparison is made between the technology needs of DHS S&T and the existing facilities, capability, experience, and personnel of DTC. Second, the strengths, weaknesses, threats, and opportunities of the problem are evaluated from the perspective of both DHS S&T and DTC. This information provides the basis for senior leaders of the organizations to determine if the evidence is available to “make it happen.”

PAGE LEFT BLANK INTENTIONALLY

CHAPTER 1

INTRODUCTION

Introduction and Background

In times of tightened budgets and confined or decreasing resources, the need for efficiency and synergy increases. In December 2009, the Office of Management and Budget (OMB) put forward the Open Government Directive. One of the key elements of this directive is to improve the effectiveness of government through collaboration. The directive specifically calls for partnerships and cooperation within the Federal Government and across all levels of government (Orszag, 2009).

In 2002, the U.S. Congress and the Executive Branch passed and signed the Homeland Security Act, which created the U.S. Department of Homeland Security (DHS). Before this act, homeland security responsibilities were scattered among 22 separate federal agencies. These agencies received over 2,000 congressional appropriations for programs, many of which were focused on the development, testing, and fielding of technologies required by their agency's users. An additional result of this act was the consolidation of the individual acquisition processes of the 22 federal agencies under the oversight of a single organization (U.S. Department of Homeland Security, 2008a).

This consolidation effort led to the creation of a new material acquisition system. Although the DHS material acquisition system is not fully formed, it is rapidly evolving. Much like other government organizations with successful acquisition systems, DHS decided to follow an acquisition life-cycle model. Within this model, the responsibility for all technology development and testing is held by the DHS Science and Technology (S&T) Directorate.

The U.S. Army has a robust and mature life-cycle acquisition system to provide effective and sustainable weapon systems and equipment for its soldiers. A critical component of the U.S. Army's life-cycle model is to conduct independent test and evaluation of technologies during their development. This information leads to an understanding of potential operational impacts and provides critical data to procurement decisionmakers. To support this effort, the U.S. Army Test and Evaluation Command (ATEC) plans, conducts, and integrates developmental testing, independent operational testing, independent evaluations, assessments, and experiments in order to provide essential information to decisionmakers. The U.S. Army Developmental Test Command (DTC), a subordinate ATEC Command, operates test centers throughout the United States, with existing facilities and equipment valued at over $4 billion. The collective talent of DTC's approximately 7,000 personnel conducts developmental testing for the U.S. Army, U.S. Department of Defense (DOD), and other agencies.

Purpose of the Study and Research Hypothesis

This research paper assesses the potential for a strategic partnership between the DHS S&T and DTC in the support of DHS' need for developmental testing. In addition, this research paper adds to the volume of knowledge on potential efficiencies and collaboration in line with the Open Government Directive.

This research tests the hypothesis that the U.S. Federal Government would benefit from a partnership between DHS S&T and DTC. This hypothesis based on two critical assumptions.

Critical Assumption 1: Not all potential relationships between the DTC test infrastructure and the DHS S&T test requirements have been fully exploited.

Critical Assumption 2: The DHS S&T test infrastructure needs are very similar to the existing DTC testing capabilities.

Overview of Methodology

The research methodology is twofold. First, a crosswalk has been done between the technology needs of DHS S&T and DTC's capabilities. A crosswalk is a detailed analysis where two separate pieces of data are evaluated for commonality. The technology user requirements are derived through a literature review of published DHS S&T technology needs (Buswell, 2009). The DTC core competencies and capabilities are drawn from DTC Regulations 10-1 and 73-1 (U.S. Department of Army, 2006). Second, a comprehensive Strengths, Weaknesses, Opportunities, and Threats (SWOT) analysis is conducted from each agency's perspective on a partnership. This analysis is done by gathering data through a literature search.

Research Limitations

Author Bias

At the time of the research, the author of this paper was an employee of DTC. The research methodology was established to remove as much bias as possible. There is no guarantee that all bias has been removed, and this must be a factor in evaluating the findings.

Matrix Diagram

The use of the 2009 DHS S&T technology needs document as the basis for the research has three limitations (Buswell, 2009). First, it only takes into account major needs areas that will drive technology developmental programs by DHS to meet gaps. For each need area, numerous technology development programs are initiated, with each creating potential solutions. Based on this information, the research may not reach the required fidelity to determine the true extent of a potential partnership. Second, use of this document creates a snapshot in time. The needs identified in this document are only valid in the near term. This is supported by the fact that the needs list has undergone three major modifications since 2003. Finally, within DHS, there are ongoing acquisition programs that are addressing need areas that do not require science and technology development but do require developmental testing. This information may not be captured within the document.

The use of core competency areas identified in DTC regulation 10-1 can also be a limitation. The competency areas by design are extremely general in nature. This research does not inspect in detail the facilities, infrastructure, and personnel that support these competency areas. The DTC facilities and infrastructure are flexible, and there is a potential that additional matches could exist that are not documented.

Strengths, Weaknesses, Opportunities, and Threats Analysis

The scope of the research required that the SWOT analysis be done at a strategic level. More detail could be derived if a tactical SWOT analysis were also completed. This tactical SWOT analysis would take into account information not easily captured or obtained through a literature search and would require different research methodologies. Efforts such as interviews or surveys would lead to a specific understanding of the needs, interests, and expectations of the two organizations.

CHAPTER 2

LITERATURE REVIEW

U.S. Army Test and Evaluation Command

In 1999, ATEC was created to consolidate the U.S. Army's developmental and operational testing responsibilities. Prior to the creation of ATEC, test responsibilities were executed by organizations under the U.S. Army Material Command. To address specific needs, ATEC is made up of three major subordinate commands: (1) DTC, headquartered at Aberdeen Proving Ground, MD; (2) U.S. Army Operational Test Command (OTC), headquartered at Fort Hood, TX; and (2) U.S. Army Evaluation Center (AEC), headquartered in Alexandria, VA. The structure is displayed in Figure 1.

Figure 1: ATEC Organizational Structure

The mission of ATEC is to plan, conduct, and integrate developmental testing, independent operational testing, independent evaluations, assessment, and experiments in order to provide essential information to the decisionmaker. Its vision is to be the premier test and evaluation organization within DoD, valued by customers and decisionmakers for providing essential information ensuring that warfighters have the right capabilities for success across the entire spectrum of operations.

The workforce of ATEC comprises 9,000 military, civilian, and contract employees who are highly skilled test officers, engineers, scientists, technicians, and evaluators involved in over 1,100 tests daily. It has locations in 17 states and an annual budget in excess of a half a billion dollars.

U.S. Army Developmental Test Command

The largest of ATEC's subordinate commands is DTC. It encompasses roughly 7,000 of ATEC's 9,000 personnel. According to DTC's figures, it possesses the largest, most diverse array of testing capabilities in the DoD. With its headquarters at Aberdeen Proving Ground (APG), MD, DTC operates a series of test centers. The test centers include Aberdeen Test Center, APG, MD; Electronic Proving Ground, Fort Huachuca, AZ; Redstone Test Center, Redstone Arsenal, AL; West Desert Test Center, Dugway Proving Ground, UT; White Sands Test Center, White Sands Missile Range, NM; Yuma Test Center at Yuma Proving Ground, AZ; cold-region capabilities at the Cold Regions Test Center, Fort Greely, AK; and tropical-region capabilities at Tropic Regions Test Center in Panama. The structure is displayed in Figure 2.

The values of customer service and stewardship of resources are essential to the execution of DTC's mission and support the vision of enabling the delivery of the best possible products to U.S. forces through rigorous developmental testing.

Major Range and Test Facility Base

The Major Range and Test Facility Base (MRTFB) is a designation given to select DoD test and evaluation test ranges. These ranges are considered national assets that provide critical infrastructure and workforce necessary to the long-term viability of the nation's test and evaluation

Figure 2: DTC Organizational Structure

capabilities. Most of DTC's test centers have been designated as part of the MRTFB. The exceptions include all of the Redstone Test Center test capabilities and select capabilities at Yuma Proving Ground and White Sands Missile Range. Based on MRTFB policy, other government agencies, local governments, private industry, academia, and allied foreign governments are permitted to use these capabilities.

However, the policy also states that the non-DoD organizations must reimburse all institutional costs associated with their test programs (England, 2007).

U.S. Department of Homeland Security

DHS was established by the Homeland Security Act of 2002. The department has a workforce of 230,000 employees working toward a common mission to ensure a homeland that is safe, secure, and resilient against terrorism and other hazards. DHS does this through five areas of responsibility: (1) prevention of terrorism and enhance security, (2) securing and management of U.S. borders, (3) enforcing and administering immigration laws, (4) safeguarding and securing cyberspace, and (5) ensuring resilience to disasters. The structure is designated in Figure 3.

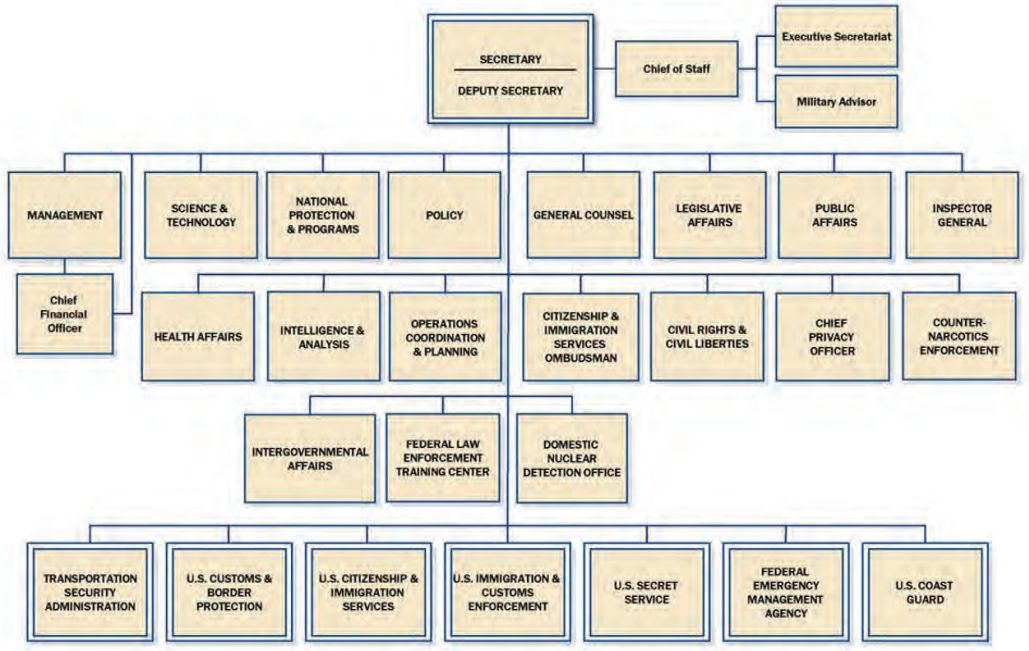

Figure 3: DHS Organizational Structure

A component of executing these responsibilities is operating an acquisition life-cycle management program. DHS uses an acquisition life-cycle framework to direct all acquisition management, support, review, and approval activities. Responsibilities for the execution of this framework are identified in the DHS Directive Number 102-01: Acquisition Management Directive (Duke, 2010).

U.S. Department of Homeland Security Science and Technology Directorate

The mission of DHS S&T is to improve homeland security by developing and providing state-of-the-art technology to the stakeholders in order to support their individual missions (Cohen, 2007). Its vision is to strengthen America's security and resiliency by providing knowledge products and innovative technology solutions for the entire homeland security enterprise. DHS S&T customers include the operating components of the DHS and state, local, tribal, and territorial emergency responders and officials. The structure is shown in Figure 4.

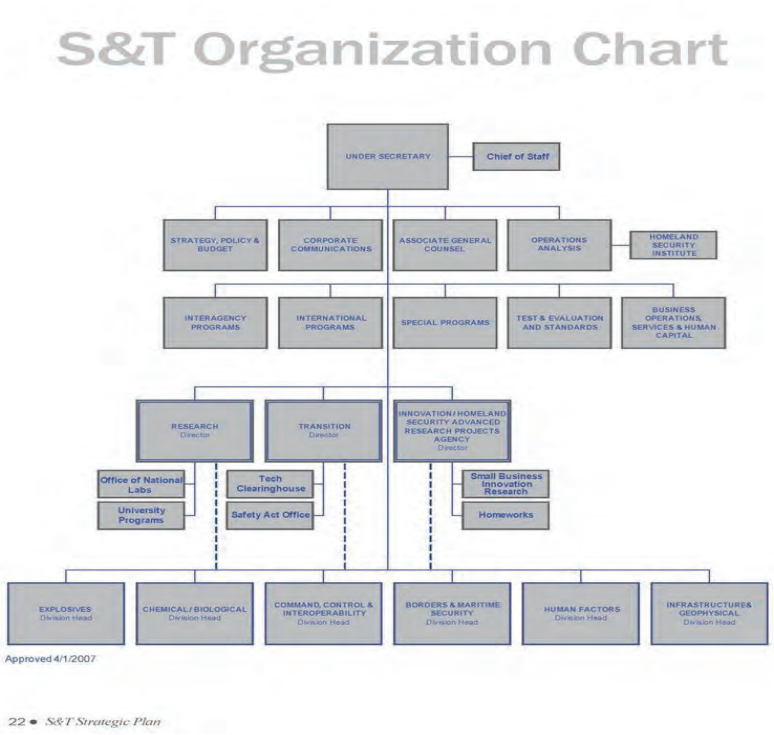

Figure 4: DHS S&T Organizational Structure

Within the DHS acquisition life-cycle framework, DHS S&T also has a critical oversight responsibility. Not only does DHS S&T deliver the critical acquisition technologies, but it also establishes the test and evaluation polices and processes for all DHS acquisitions (Duke, 2010). This includes providing timely and accurate information to stakeholders in order to determine impacts to programmatic performance, schedule, and financial risks (Hale, 2005).

Practical Use of Strengths, Weaknesses, Opportunities, and Threats Analysis

It is commonly agreed that SWOT analysis has become an integral component of strategic planning for academia, business, and the government (Everett & Duval, 2010). There are many examples of organizations using SWOT analysis for internal purposes. An example of multiple partners using the SWOT analysis to determine if a strategic partnership was in their best interest is described and published by Ryynänen and Jansson (**2007)**.

Ryynänen and Jansson conducted a case study on a group of Finnish maritime companies looking to identify opportunities and challenges to a partnership. The maritime companies believed that through strategic cooperation, they could enter a new market that previously would have been unavailable. With the support of an organizational development practitioner, they determined the main challenges and opportunities. They categorized, detailed, and ran the information through a SWOT analysis to determine the benefits and issues with the partnership (Ryynänen & Jansson, 2007). This case study demonstrates the feasibility and usefulness of a SWOT analysis in assessing strategic partnerships.

Organizational and Strategic Planning

Strategic planning efforts are common among organizations, including agencies within the Federal Government. Based on internal and external initiatives, organizations frequently analyze methods of operating at greater efficiencies. These efficiencies can often be tied into the strategic plan of an organization.

Both DHS and DHS S&T periodically publish strategic plans (Chertoff, 2008). These plans are widely distributed and publicly available. The DHS S&T plan builds off the DHS organizational strategic plan. This level of planning is required and beneficial in such a young organization to communicate the mission and vision and lay out both the short- and long-term goals of the organization. In regard to this research, there is no discussion of partnership with DTC in the DHS S&T strategic plan (Cohen, 2007)

On the other hand, DTC does not have a publicly published strategic plan. The organization is much more mature and relies on regulations and guidance to guide its future posture. The U.S. Army's acquisition system is solidly established, and DTC's role within the system is well-defined. The research for this paper did not uncover evidence of DTC planning for a partnership with DHS S&T.

History of Testing Partnerships

Working in partnership is not a new concept for DHS S&T and DTC. Historically, DHS S&T has used DTC tests center's status as MRTFB as a mechanism to support its developmental testing and training needs. The efforts have been typically transactional in nature and not based on long-term memorandums of understanding and agreements. DHS S&T and DTC test ranges have worked together to test numerous technologies in the DHS S&T portfolio. Areas of collaboration include explosive detection, chemical detection, survivability, nonlethal munitions, and robotics (International Test and Evaluation Association, 2007).

The most robust partnership occurs between the U.S. Army Dugway Proving Ground and DHS S&T to support the testing of technologies in the biological and chemical threat portfolio. U.S. Army Dugway Proving Ground is uniquely qualified to support large-scale developmental testing in this area and has supported DHS S&T consistently since its inception.

CHAPTER 3

RESEARCH METHODOLOGY

Research Design

The research methodology used to assess the hypothesis is twofold. The first methodology is an analysis between the technology needs of DHS S&T and the test capabilities of DTC. This is done using a matrix diagram where two sets of data are cross-walked and analyzed for areas of overlaps. Second, a strategic analysis from the perspectives of both DTC and DHS is completed. This is done using a SWOT strategic planning model.

Matrix Diagram Background

There are numerous ways to demonstrate the relationship between separate pieces of information. The American Society of Quality advocates seven management and planning tools to aid in developing these relationships. The seven tools are the affinity diagram, relations diagram, tree diagram, process decision program chart, arrow diagram, matrix diagram, and matrix data analysis (Tague, 2005). The complexity and useful area of each tool are described in Table 1.

Table 1: American Society of Quality Management and Planning Tools

Complexity	Tool	Usefulness
Highest	Affinity diagram	Brainstorming and consensus
	Relations diagram	Cause and effect
	Tree diagram	Logic-based problem solving
	Process decision program chart	Identifying best solution
	Arrow diagram	Resource planning
	Matrix diagram	Determining interrelated factors
Lowest	Matrix data analysis	Quantitative analysis

The most useful tool for this research paper is the matrix diagram. The matrix diagram can be used to determine interrelated factors (Levesque & Walker, 2007). Within the family of matrix diagrams, there are different formats: L, T, Y, X, C, R, and roof-shaped (Tague, 2005). The appropriate format to select is based on the number of data points and groups to be compared. The L-shaped matrix diagram relates two groups of items to each other and is most applicable to the scope of this research paper (Levesque & Walker, 2007).

Use of Matrix Diagram in This Research

This research paper conducts a matrix diagram analysis to determine the overlap between the technology needs of DHS S&T to the test capabilities of DTC. For the purposes of this research paper, it is more important to determine if DTC in general can provide the test support to DHS S&T rather than which specific test center can provide the support. To narrow the scope, only areas currently identified by DTC as core capabilities are evaluated.

Consolidation of U.S. Department of Homeland Security Science and Technology Needs

The dynamic world and external environment drives the need for continued technology development. DHS S&T is responsible for developing those technologies to respond to known and emerging threats. In both a financial resource and time-constrained environment, the homeland security technology development community requires guidance on which problems to address. DHS S&T periodically publishes a document outlining the high-priority technology needs to give the academic, laboratory, and private industry sectors insight into the most pressing requirements. The latest is version 3.0 where technology needs are bundled underneath one of 13 newly established Capstone Integrated Product Teams (IPT) (Buswell, 2009). These IPTs can be found in Table 2.

Table 2: DHS S&T Capstone IPTs

Capstone IPTs	
Border Security	Cargo Security
Chemical and Biological Defense	Counter Improvised Explosive Device (IED)
Cyber-Security	First Responder
Incident Management	Information Sharing
Infrastructure Protection	Interoperability
Maritime Security	People-Screening
Transportation Security	

In total, DHS S&T has identified 99 high-priority technology needs. Each one is assigned to a Capstone IPT. The technology needs identified by DHS S&T serve as the baseline for the vertical component of the L-shaped matrix design.

Consolidation of U.S. Army Developmental Test Center Capabilities

Test and evaluation facilities, capabilities, and infrastructure are expensive to maintain and fully fund. Efforts are made to ensure that MRFTB members work at peak efficiency in order to maximize their budgets. To keep duplication at a minimum, individual test centers are given primary capability responsibilities for specific areas of developmental testing. Other test centers can be given reinforcing or supplemental roles in those developmental test areas to help in times of excess workload. To manage this effort, DTC promulgated a series of regulations to define the missions and major capabilities of each test center. These regulations are listed in Table 3.

Table 3: DTC Mission and Capability Regulations

DTC Regulation	Title	Test Center Location
10-3[a]	Mission and Major Capabilities of the U.S. Army Aberdeen Test Center	APG, MD
10-4[b]	Mission and Major Capabilities of the U.S. Army Redstone Test Center	Redstone Arsenal, AL
10-5[c]	Mission and Major Capabilities of the U.S. Army Yuma Proving Ground.	Yuma, AZ
10-6[d]	Mission and Major Capabilities of the U.S. Army White Sands Missile Range	White Sands Missile Range, NM
10-7[e]	Mission and Major Capabilities of the U.S. Army Dugway Proving Ground	Dugway, UT
10-9[f]	Mission and Major Capabilities of the U.S. Army Electronic Proving Ground.	Fort Huachuca, AZ

[a]U.S. Department of the Army (2009a)
[b]U.S. Department of the Army (2009d)
[c]U.S .Department of the Army (2009f)
[d]U.S. Department of the Army (2009e)
[e]U.S. Department of the Army (2009b)
[f]U.S. Department of the Army (2009c)

In the appendix of these DTC regulations is a consolidated L-shaped matrix diagram comparing the core commodity area test capabilities requirements against the test centers that hold primary, reinforcing, supplemental Level One, or supplemental Level Two capabilities. DTC has identified a total of 43 major capability areas. The 43 capabilities areas identified in the regulations are used in this research as the horizontal component of the L-shaped matrix.

Strengths, Weaknesses, Opportunities, and Threats Analysis Background

The use of a SWOT analysis is a strategic planning tool in the organizational change and development communities (Coman & Ronen, 2009). The SWOT analysis is an accepted framework to begin any organizing thoughts on a particular problem (Sluismans, Lommelen, & den Hertog, 2010). Examples of uses for SWOT include business planning, marketing, competitor evaluation, strategic planning, decisionmaking, product development, brainstorming, and research reports.

SWOT analysis was developed at the Stanford Research Institute by Albert Humphrey in the 1960s. Since then, it has been well researched and validated as a legitimate data analysis tool (Sluismans, Lommelen, & den Hertog, 2010). There are four components of the SWOT analysis. Each component is analyzed against the problem statement and displayed in a four-square chart as shown in Figure 5.

Figure 5: SWOT Analysis

Use of Strengths, Weaknesses, Opportunities, and Threats Analysis in this Research

This research paper uses a SWOT analysis to determine the feasibility of a strategic partnership between the DTC and DHS S&T. In the case of strategic partnerships, each organization would have its own interest, expectations, and requirements **(**Ryynänen & Jansson**, 2007).** Therefore, two SWOT analyses are required to investigate the issue from each organization's perspective. To the extent possible, the data addressing each area of the analysis is gathered from published sources.

Strengths

Strengths are all of the components and qualities that allow the organization to support the problem statement. The strengths are the basis to continue or grow in the success of the organization. These strengths can be as tangible as facilities or as intangible as intellectual capital. Strengths are internal to the organization and can therefore be controlled. They provide positive reinforcement to the planning effort.

Weaknesses

Weaknesses are all the components and qualities that will prevent or hinder the organization from supporting the problem statement. Weaknesses must be overcome because they prevent the success of the organization. They are internal to the organization and are therefore controllable. They are limitations placed on the planning effort.

Opportunities

Opportunities are advantages presented by the external environment from which the organization can benefit. Opportunities can be leveraged to support the problem statement and gain an advantage. Opportunities are often short-lived and fleeting because they are not under the control of the organization. If they are not recognized, they can quickly disappear.

Threats

Threats are issues that are presented by the external environment that hinder or harm an organization in gaining an advantage. Threats can make all planning and support of the problem statement unproductive. Threats are external to the organization and are uncontrollable. They serve as cautionary indicators that may have negative impacts on addressing the problem statement.

CHAPTER 4

DATA ANALYSIS AND RESULTS

Matrix Diagram Analysis

The results of the crosswalk of 99 DHS S&T technology needs and the 43 DTC test capabilities using the matrix diagram is found in Appendix A. The most striking result is that there is not an obvious direct match between DHS S&T technology needs and a DTC capability in 47 of the 99 needs.

When reviewing the matrix diagram results, it is clear that there is a significant difference among the relative fit between the 13 DHS Capstone IPTs technology needs and the DTC capabilities. Since only 53 percent have direct matches, a second analysis is required. The second analysis evaluates the relative fit of each Capstone IPT as a whole against the test capabilities of DTC. A determination is made whether the fit between the focus areas and the competency is significant, partial, or minimal.

Border Security Capstone Integrated Product Team Needs

The Border Security Capstone IPT addresses technology gaps in threat detection, identification, apprehension, and law enforcement at checkpoints and along the U.S. borders. The technology developmental testing needs within this IPT significantly match the core capabilities of DTC.

The technologies developed for this IPT include nonlethal and detection systems. Similar technologies have been tested by DTC for use by the warfighter, and have military-like uses. A specific technology need not addressed by a DTC core test capability is the ability to test improved analysis and decisionmaking tools.

Cargo Security Capstone Integrated Product Team Needs

The Cargo Security Capstone IPT addresses the technology gaps in the system of systems approach to manage the safe operation of the U.S. exchange of goods and supplies. The technology developmental testing needs of this IPT significantly match the core capabilities of DTC.

The technologies developed for this IPT include scanners, detectors, and inspection devices. The representative threats required to conduct developmental testing are not readily available in private industry. DTC can leverage access to these threats based on the similar use in military system testing. The technology need not addressed by a DTC core test capability is tracking domestic high-threat cargo.

Chemical and Biological Defense Capstone Integrated Product Team Needs

The Chemical and Biological Defense Capstone IPT addresses the technology gaps in detection, mitigation, protection, deterrence, recovery, and understanding of chemical and biological attacks. The technology developmental testing needs of this IPT partially match the core capabilities of DTC.

The needs for this IPT are numerous and diverse, spanning the range of consequence modeling to decontamination technologies. There are unique facilities and capabilities available in this DTC competency area, especially in the detection and decontamination need areas. The technology needs not addressed by a DTC core test capability are in risk assessment, data fusion, national architecture, consequence analysis, and incident characterization. These areas can be addressed by U.S. Army organizations outside of DTC.

Counter Improvised Explosive Devise Capstone Integrated Product Team Needs

The Counter Improvised Explosive Devise (IED) Capstone IPT addresses the technology gaps found in the IED attack network. Defeating the IED network requires the ability to disrupt all phases of an IED attack. This requires (1) understanding the enemy, (2) predictive tools regarding attacks, (3) methods to detect, (4) the means to dispose of threats, and (5) survivability in case of detonation. The technology developmental testing needs of this IPT significantly match the core competencies of DTC.

The technology needs of this IPT mirror those that are developed and tested for use by the warfighter. DTC has experience and facilities designated for testing these technologies. The technology needs not addressed by a DTC capability are in the areas of the testing of novel computational and predictive behavioral models. These areas can be addressed by U.S. Army organizations outside of DTC.

Cyber-Security Capstone Integrated Product Team Needs

The Cyber-Security Capstone IPT develops technologies and processes in support of information sharing and protection. This life-cycle IPT reviews critical information infrastructure required to secure the U.S. cyber-backbone. The technology developmental testing needs of this IPT minimally match the core capabilities of DTC.

DTC conducts software and network system testing for U.S. Army weapons and communication systems, but the majority of cyber-efforts are completed by the U.S. Army and Joint Cyber Commands.

First Responder Capstone Integrated Product Team Needs

The First Responder Capstone IPT addresses the technology gaps in the public-service sector of homeland security. The majority of these technologies require large-scale commercial acquisitions by federal, state, and local governments to equip and prepare the first-responder community. The technology developmental needs of this IPT partially match the core capabilities of DTC.

The nonlethal and detection technology needs of this IPT are similar to those tested for use by the warfighter. DTC has the ability to provide the broad environmental test requirements for the commercial systems. Testing of command and control systems is also a core competency of DTC. The technology needs not addressed by a DTC core capability area are in the areas of training, predicting criminal activity, credential identification, and information management. Some of these areas can be addressed by U.S. Army organizations outside of DTC.

Incident Management Capstone Integrated Product Team Needs

The Incident Management Capstone IPT addresses technologies required for situational awareness and emergency response capabilities while executing a disaster-relief operation. The technology needs focus on simulation-based training, situational command-and-control awareness, and logistics management. The technology developmental needs of this IPT minimally match the core capabilities of DTC.

The personnel monitoring needs are similar to technologies tested by DTC for use by the warfighter. The technology needs not addressed by DTC are in the testing of simulation training technologies, logistics management tools, and an incident management enterprise system. These areas can be addressed by U.S. Army organizations outside of DTC.

Information Sharing Capstone Integrated Product Team Needs

The Information Sharing Capstone IPT develops technologies and processes to support all aspects of information and data. This can include analyzing, sharing, gathering, and protecting. The goal is to develop a means to fuse all data securely across all jurisdictions to facilitate coordination and knowledge sharing. The technology development needs of this IPT minimally match the core capabilities of DTC.

DTC developmental test capabilities include command and control, but the scope and scale of the technology needs are outside of DTC's area of expertise. These areas can be addressed by U.S. Army organizations outside of DTC.

Infrastructure Protection Capstone Integrated Product Team Needs

The Infrastructure Protection Capstone IPT prepares and responds to threats against critical infrastructure assets of the United States. The technical solutions developed in this area provide interim mobile backup systems to support the infrastructure of the impacted area. The technology development needs of this IPT partially match the core capabilities of DTC.

Areas of overlap include blast analysis and mobile utility services. These technology needs are addressed by DTC for the warfighter. DTC does not have developmental test capabilities in the areas of levee monitoring, analytical infrastructure sector predictive tools, or decision support systems. These areas can be addressed by U.S. Army organizations outside of DTC.

Interoperability Capstone Integrated Product Teams

The Interoperability Capstone IPT supports the sharing of information between technology solutions in radio communication, data exchange, networks, and public alert systems. There are two components to this IPT: (1) technology development and (2) standards development. The technology development needs of this IPT partially match the core competencies of DTC.

DTC has extensive developmental test capabilities in for communication systems and interoperability. These technologies are used on the battlefield by the warfighter to communicate across services and weapon systems. The standard development technology needs do not match with DTC core capabilities.

Maritime Security Capstone Integrated Product Team Needs

The Maritime Security Capstone IPT focuses on border issues of the U.S. waterways and coasts. The IPT concentrates on communication, sensors, and surveillance technologies. The technology development needs of this IPT partially match the core capabilities of DTC.

The detection of contraband materials, nonlethal compliance, and tracking of material are core competencies. The technology needs better addressed by other organizations include long-range radar and wide-area surveillance for maritime applications.

People-Screening Capstone Integrated Product Team Needs

The People-Screening Capstone IPT is developing methods and technologies used to identify individuals in an accurate and noninvasive manner. This provides the capability to analyze threats and understand individuals' identities and backgrounds. The technology development needs of this IPT partially match the core capabilities of DTC.

The needs of the warfighter for these technologies have lead to the developmental testing capability. This is a newer capability and focuses on military applications instead of commercial applications. The areas that DTC does not address are data fusion for real-time assessment, behavioral predictors, and DNA identification.

Transportation Security Capstone Integrated Product Team Needs

The Transportation Security Capstone IPT is responsible for developing a system of systems technology suite to support the safety and security of the movement of people and material across the United States. This makes all modes of transportation safe while allowing the required freedom of movement that is necessary in this society. The technology development needs of this IPT significantly match the core capabilities of DTC.

The representative threats required to conduct developmental testing are not readily available in private industry. DTC can leverage access to these threats based on similar use in military system testing.

Matrix Diagram Results

The matrix diagram results can be best summarized graphically in three ways. Figure 6 illustrates the percentage of DHS S&T technology needs addressed by DTC capabilities. Table 4 illustrates the relative match between the DHS Capstone IPTs and the DTC capabilities. Appendix A shows the entire matrix diagram and matches between the technology needs of DHS S&T and the capabilities of DTC.

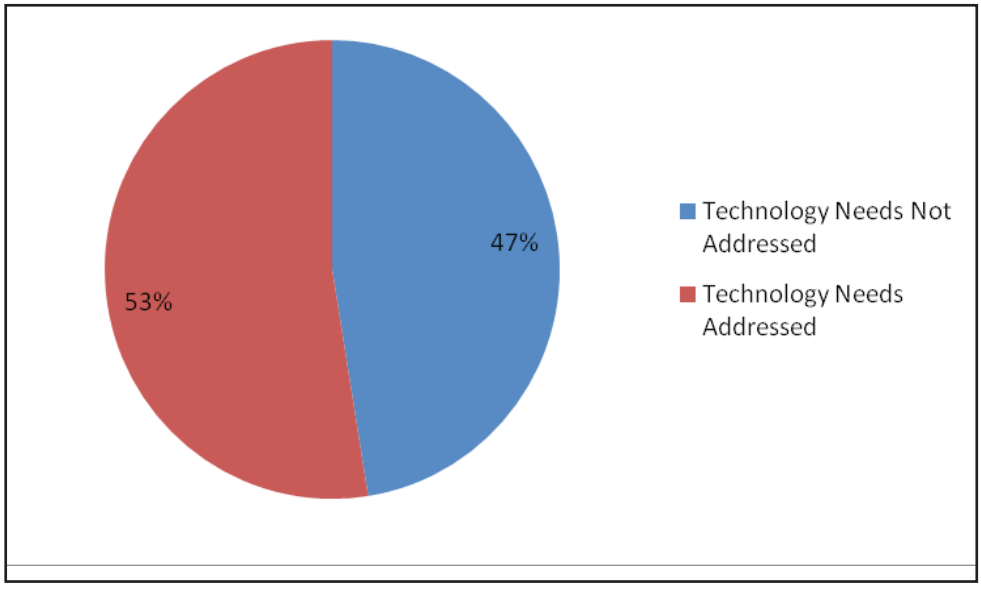

Figure 6: Percentage of Needs vs. Capabilities

Table 4: Capstone IPT Level of Match

Capstone IPT	Capability Match
Border Security	Significant
Cargo Security	Significant
Chemical and Biological Defense	Partial
Counter IED	Significant
Cyber-Security	Minimal
First Responder	Partial
Incident Management	Minimal
Information Sharing	Minimal
Infrastructure Protection	Partial
Interoperability	Partial
Maritime Security	Partial
People-Screening	Partial
Transportation Security	Significant

Strengths, Weaknesses, Opportunities, and Threats Analysis

The results of a SWOT analysis are highly influenced on the question that is investigated. In order to evaluate the hypothesis, this research investigates the question, "Should DHS S&T and DTC enter into a strategic partnership?" The SWOT analysis is different depending on the perspective in which the individual answers the question. Therefore, the results from both parties' perspective are provided. The summary SWOT analysis can be found in Appendix B.

Strengths from the U.S. Department of Homeland Security Science and Technology Perspective

Understood Test Standards

The majority of DHS technology acquisition programs rely on commercially off-the-shelf technologies. The technology requirements are also well-defined by the users. The scale of acquisition purchases across the nature makes it a competitive market for the system developers. In addition, this allows DHS S&T to establish standards for these technologies to be tested against. Having clear standards for which commercial items can be judged, the test planning process becomes much simpler.

DHS has developed a partnership with the American National Standard Institute to manage and maintain a homeland security standards database. This database catalogs all the approved homeland security standards resulting from the standards working groups. DHS' four standards working groups are: (1) chemical, biological, radiological, nuclear, and explosive (CBRNE) countermeasures, (2) emergency preparedness and response, (3) border and transportation safety, and (4) standards process and infrastructure development (U.S. Department of Homeland Security, 2008b). In addition, DHS uses other voluntary consensus standards coming from the Interagency Committee on Standards Policy and the DHS standards counsel (Coursey, 2008).

Partnership Promotion

The leadership of DHS is promoting a culture of cooperation and partnership. This is demonstrated through organizational vision statements and publications that specifically identify the need for coordination among federal agencies. This support from senior management can drive a willingness to seek expertise externally.

DHS management recognizes that the agency does not work in a vacuum and that working as an integrated response team is the only way to deal with the whole spectrum of homeland security scenarios. An example of this outreach is the DHS solicitation of comments from the DoD during development of the DHS Strategic Plan (Chertoff, 2008).

Flexibility

DHS has shown its ability to be flexible in adapting to the emerging needs of the agency. It has reorganized multiple times and continues to stabilize the organization as time advances. As an organization, DHS' size and diverse mission allows it to shift resources and personnel to meet emerging needs and threats.

The political landscape is extremely difficult for DHS S&T. For the most part, it has shown the ability to adjust and answer criticism. Its publicly available literature acknowledges changes in the environment and actions that are undertaken by DHS to make the adjustment.

Existing Partnerships

The flexibility and available funding of DHS has lead to a wide cast of partners throughout academia, private industry, and other government agencies. These organizations have identified an opportunity to collaborate with DHS S&T to provide services that were not available internally. This network of partners allows DHS S&T to seek the expertise of others to support its technology development.

In many cases, there are dual-use opportunities for the technologies being developed for DHS S&T. By identifying who holds the institutional knowledge on a technology commodity area and partnering with them, DHS S&T shortens the learning curve within the system's development. Seeking and maintaining partnerships is a core competency of DHS S&T.

Weaknesses from the U.S. Department of Homeland Security Science and Technology Perspective

Acquisition Workforce

A consistent theme in numerous U.S. Government Accountability Office (GAO) and internal DHS reports is the struggle to develop the DHS acquisition workforce. The acquisition workforce in DHS is currently growing, but is only concentrated on training, hiring, and developing the contracting specialty. Gaps remain in the other core competencies such as testing, logistics, and systems engineering (U.S. Government Accountability Office, 2009).

To counterbalance this problem, DHS S&T is developing a test and evaluation career field, but the workforce's instability has lead to little gains in this area. To this point, the DHS S&T strategic plan states that, as those in the science and technology career field get up to speed, they will become highly vulnerable to being poached for positions of higher responsibility in DHS and the government outside the DHS S&T community (Cohen, 2007).

Acquisition Program Longevity

Creation of DHS resulted in a need to combine numerous acquisition programs of the member agencies. No single existing acquisition program could satisfy the needs of the entire DHS enterprise, leading to a lack of integration of the acquisition system across the homeland defense enterprise (U.S. Government Accountability Office, 2007a). The relative instability of DHS as a whole is evidenced by the fact that in the first five years of existence, seven organization charts were developed to delineate the DHS structure (U.S. Department of Homeland Security, 2008a).

Combining systems was a monumental process that continues to be shaped and refined as issues are uncovered. Although DHS is working toward competency, there is currently limited accountability in its acquisition programs (U.S. Government Accountability Office, 2007b).

Lack of Coordinated Test and Evaluation

Understanding the need to get a better handle on the test and evaluation issues, DHS created the Office of Test and Evaluation. The office only handles policy issues, leaving no single entity to manage test facilities or coordinate testing activities (Coursey, 2008). There is no independent organization to provide acquisition authorities with an evaluation of the capabilities and limitations of the technology under test.

Limited U.S. Department of Homeland Security Test Infrastructure

Program managers executing DHS acquisition programs can select from a host of test facilities to execute their testing requirements. There is a limited organized DHS test infrastructure. This requires DHS to rely on the other test facilities to execute its developmental test work. These facilities can be internal DHS laboratories, U.S. Department of Energy (DOE) laboratories, MRTFBs, academia, or private industries (Coursey, 2008).

Without control over the test facilities, there is limited control over schedule, costs, availability, or priority. To combat this, there is also a drive from member agencies of DHS to develop their own facilities. Unfortunately, this may cause duplication of existing federal and commercial facilities and does not have the full support of the DHS leadership (Coursey, 2008).

Opportunities from the U.S. Department of Homeland Security Science and Technology Perspective

External Lessons Learned

External organizations are helping DHS develop its long-term strategies for the acquisition system as well as a DHS-unique acquisition workforce. The Defense Acquisition University is building a training and certification program tailored specifically to the needs of DHS. This focused coursework will develop the core competencies of the DHS acquisition workforce (U.S. Government Accountability Office, 2009). Until the DHS certification criteria are completely established, the DoD system is being used as an interim certification process.

The DHS acquisition management system also will benefit from the years of development and lessons learned by DoD. This information is codified in DoD Directive 5000.01, The Defense Acquisition System and DoD Instruction 5000.02, Operation of the Defense Acquisition System (U.S. Government Accountability Office, 2009).

Leveraging Partnership Programs

If other government agencies are developing technologies that meet common needs, there is an opportunity for DHS to partner or leverage to reduce program costs and schedules. Resources can be focused on meeting the unique needs of DHS. In addition, if DHS is not required to build or maintain its own test infrastructure, it can use those resources on technology development or fielding instead of a test workforce or facilities.

The Technical Support Working Group (TSWG) is an interagency organization that coordinates interagency governmental research and development (R&D) programs. DHS is an active participant in TSWG, providing an opportunity not only to coordinate technology research and development, but also to establish relationships to address testing needs. Participation in interagency groups supports the U.S. Army Science and Technology Board recommendation that DoD aid DHS in developing appropriate planning and execution of joint programs (Carafano, Czerwinski, & Weitz, 2006).

Built-in Objectivity

During after-action reviews of DHS major acquisition programs, multiple highly visible mistakes during its testing phase were identified. Some of these mistakes were clear violations of protocol and were driven by either inexperience or loss of objectivity by the DHS program office attempting to develop the technology (Hite, 2010). This appearance of conflict of interest is a political problem for DHS.

Use of an outside organization to support the independent test and evaluation of programs can serve as a system of checks and balances for DHS. In addition, the project manager's ability to violate test protocols would be limited if DHS did not have direct control of the test execution. DHS could also leverage the experience of the test organization to support test planning and scope.

Relationship Formalization

There is a potential for DHS S&T to gain greater efficiencies by establishing formal relationships with an outside test organization. A memorandum of agreement can identify the specific roles and responsibilities so all parties have a clear understanding of the partnership. Financial arrangements could be made that benefit both parties and result in cost savings. The benefits could include steady workflow, dedicated facilities, dispute resolution, and a mechanism to spur communication.

In addition, DHS has unique test capabilities from which other organizations could benefit. Facilities and test capabilities operated by DHS such as the DHS Chemical Security Analysis Center, National Biodefense Analysis and Countermeasures Center, National Urban Security Technology Laboratory, Plum Island Animal Disease Center, and Transportation Security Laboratory could be made available to other organizations. This reciprocity could prevent further duplication of efforts and serve as an opportunity to partner technology development or dual-use applications.

Threats from the U.S. Department of Homeland Security Science and Technology Perspective

Oversight

Numerous reports questioning the DHS acquisition community and the testing of its major test programs such as deepwater, secure border initiative, and container security have been published by GAO (U.S. Government Accountability Office, 2007b). The acquisition system is compared against the DoD as a benchmark (U.S. Government Accountability Office, 2009). It is acknowledged that acquisition program development is not an easy task. It is agreed that it could take multiple years to be fully implemented. This time lag may lead to more oversight and continued scrutiny.

Being a new, large, politically visible organization, DHS and its programs receive massive oversight. Eighty-six congressional committees provide oversight and impose mandatory reporting requirements. With this amount of oversight, the political influence of decisionmaking is extremely unstable and inefficient. Oversight is identified by DHS as one of its most dangerous obstacles in achieving its mission (U.S. Department of Homeland Security, 2008c).

Economic Factors

The national political climate and the state of the national economy have the potential to impact funding to all government organizations. There is a potential for budgetary freezes or cuts, especially in discretionary spending. The impact of this on DHS S&T is unknown. It is recognized that in periods of economic struggle, the DHS state, local, and private industry partners will be likelier not to fulfill their long-term commitment to financing homeland security efforts (U.S. Department of Homeland Security, 2008c).

It is safe to assume that DHS S&T will not be immune from any budgetary impacts. These impacts would trickle down to any established partners. Within DHS, technology development and testing would be vulnerable to cuts, especially regarding high-risk or over-budget programs.

Impact to Current Partnerships

The existing relationships between DHS and other research centers have been developed over time, and those partners have become reliant on receiving that funding. In order to support DHS, many organizations have made long-term investments and increased capabilities. This is especially true in the case of the Department of Energy (DOE) National Laboratories.

Although the DOE National Laboratories have test capabilities, they are also tied to the development of the technology. The threat to these laboratories would be a reduction in workload and funding if a portion of the acquisition they support is taken away (U.S. Government Accountability Office, 2004).

Culture

When two organizations with similar but not exact missions come together, there is a chance for a difference in culture. This has been observed in joint programs where DHS' perspective on technology application comes from a law-enforcement application and the U.S. Army's perspective comes from a military application.

In addition, the organizations have two different leadership structures. Terminology, values, and processes may also not be synchronized. The coordination of these cultures is difficult and may not be the highest priority for either organization. This can lead to a failed partnership.

Strengths from the U.S. Army Developmental Test Command Perspective

Existing Test Capabilities

As demonstrated by the matrix design crosswalk, DTC has significant facilities and capabilities to support DHS testing needs. Half of the technology needs of DHS S&T can be directly supported with little or no difficulty. The $4 billion investment in developmental test facilities and instrumentation provides a solid base and flexibility so customers' unique requirements can be solved. The customer diversity of DTC is a testimony to its diverse capabilities and ability to meet test needs.

The business management processes of DTC are straightforward. The organization has standard rates, provides estimates, and only charges for direct and overhead costs solely associated with the test.

Mature and Experienced Acquisition Workforce

The workforce of DTC is recognized for its quality and expertise in the field. To this point, there is a concern about the number of retirement-eligible individuals in the test and evaluation career field and in the MRTFB workforce (Undersecretary of Defense for Acquisition, Logistics, and Technology, 2008). There has been a systematic attempt to fix this issue by expanding the DoD acquisition workforce, establishing mentoring, and implementing contractor-to-government insourcing.

This workforce can support the test customer by providing input on the test planning process, translating system requirements into a design of experiment, and supporting data analysis (Undersecretary of Defense for Acquisition, Logistics, and Technology, 2008). A partnership between the tester and the customer can lead to a more robust product and reduce program risk.

Evaluation Support

One of the critical components of testing is evaluation. Testing may gather the required data for the customer, but the evaluation of the results is critical to its understanding. DTC has a symbiotic relationship with the U.S. Army Evaluation Command to provide this service. Providing both independent test and evaluation can be a benefit to DHS S&T.

Credibility

A core value of ATEC is to provide unbiased information and recommendations to its customers. This has led to its reputation as an organization of ethical, independent testers. The other two core values of ATEC are teamwork and cooperation. These values ensure that the test community does not become a roadblock and does everything in its power to produce safe and effective products for the warfighter.

Weaknesses from the U.S. Army Developmental Test Command Perspective

No Existing Formal Relationship

Formal relationships have been developed between the DOE National Laboratories and DHS S&T to provide the majority of their testing and R&D support. There is no formal agreement between DHS and DTC in the form of memorandum of agreement or interagency agreements. There is also no discussion about the use of DTC test ranges in the DHS R&D partnership group guidance document (Cellucci, 2010).

Past efforts have been done on a pay-for-test-service manner. Although the leadership has identified the need to work with external federal agencies, it is clear this has not been fully adopted by the workforce. There are opportunities that are being overlooked and missed.

Operational Testing

Developmental testing is one part of the overall DHS test and evaluation strategy. Any successful test and evaluation strategy requires both developmental and operational testing capabilities. The responsibility for operational testing lies with the OTC. Although OTC and DTC both answer to the same higher headquarters, ATEC, there is a difference between the operational testers and the developmental testers.

The DTC test ranges and officers do not specialize in operational testing, and any operational test events that they run would be outside of their core capability. It would not be practical for DTC to provide cradle-to-grave test support services to DHS S&T without the support of its sister organizations. Operational testing would still be required to be completed by another organization.

Financial Stability

This long-term threat will decrease the flexibility of funding of an acquisition system. Traditionally, testing is one of the first things to be cut (U.S. Department of Homeland Security, 2008c). Historically, DTC struggles with workload requirements, budgeting for that workload, and determining the best means to allocate money to the test centers (Cast, 2010). With the scope of the DTC budget, it is often a target by external organizations to be raided for unfunded requirements.

Testing is often misunderstood, and the infrastructure and human capital requirements are underestimated. Communication to the U.S. Army and DoD senior leadership is required to continue to protect the funding requirements (Cast, 2010)

Existing Workload

Since the outbreak of the conflicts in Southwest Asia in the early 2000s, the DTC workload has grown to meet the needs of the warfighter. Although the workforce has grown, workforce expansion has not paralleled this continual growth. The difference between the workload and the size of required workforce is being absorbed through the use of overtime and multiple shifts (Cast, 2010). This is not sustainable.

Additional workload in the DTC test centers can exacerbate this issue. The impact of this workload may stretch the facilities and workforce too far. In addition, there may be a requirement to modify or reconfigure test facilities to meet the DHS S&T testing needs. The support elements required to do this may not be readily available based on existing mission requirements.

Opportunities from the U.S. Army Developmental Test Command Perspective

Support for Partnerships

The DoD strategy document for homeland defense calls for DoD to share experience and technology across military and civilian boundaries (England, 2007). This document provides the broad guidance necessary to support a partnering relationship between organizations. The U.S. Army Science and Technology Board called for DoD and DHS to collaborate on experimentation, testing, review, and standardization of technologies. It recommended that they should build a joint forum at the assistant secretary level (England, 2007). There are also opportunities to collaborate to ensure interoperability between the U.S. Army and the civil authority within the homeland security arena.

Diversity of Workload

Partnership with DHS can create a steady workload coming into DTC test ranges. As the budgetary dollars become increasingly scarce and the number of U.S. Army weapons systems program decreases, there is an opportunity to keep the infrastructure and workforce engaged. This could also support potential downturns in core funding.

Testing for DHS S&T can also serve as an opportunity to broaden the experience of the DTC test directors into new commodity areas. Test directors who are cross-trained and have multiple skills provide DTC with greater flexibility when missions or workload shift.

Increased Communication and Coordination

DTC can coordinate with the newly developed DHS Interagency Programs Division. This DHS resource is responsible for coordinating with other U.S. executive branch agencies to increase collaboration and avoid duplication of effort. When DTC identifies opportunity, this is a means to communicate with DHS (U.S. Department of Homeland Security, 2008b).

There are multiple political and financial benefits when organizations work together. As government organizations, it is their responsibility to work both effectively and efficiently to protect the taxpayer interests.

New Infrastructure

The creation, maintenance, and upgrade of test infrastructure, facilities, and instrumentation are expensive. Instrumentation must be state of the art to test the latest technologies. When the newly developed technology outpaces the instrumentation and facilities used to test its capabilities, validity of the test results becomes questionable.

When multiple organizations partner, funding can be leveraged to develop dual-use test facilities and infrastructure. This will not only keep the capabilities relevant, but will demonstrate fiscal responsibility for the taxpayer. DHS S&T has partnered with other U.S. Army organizations to develop facilities that can satisfy both organizations' missions.

Threats from the U.S. Army Developmental Test Command Perspective

U.S. Department of Defense Efficiency Efforts

In 2010, the Secretary of Defense announced an initiative to find efficiencies within all levels of DoD. This effort has lead to a review of processes, funding, and requirements throughout DoD. The effort is being undertaken to cause a "culture of savings" and to reform the DoD business practices. The process is not to return the $100 billion saved over the five-year budget cycle to the federal government, but to reinvest $100 billion in high-priority military capabilities. In practical terms, any savings found will likely become a permanent cut (Maze, 2011).

This focus on reducing overhead and focusing on force structure and upgrade is not necessarily compatible with partnering with external organizations. There may be a potential to increase the overhead to support the effort. In addition, the growth in workload could make the DTC budget larger than what the DoD budget analysts believe is necessary. This will appear to observers as running contrary to the efficiency initiative. The efficient effort may have a significant impact on the partnership between DHS S&T and DTC.

Reliance on U.S. Department of Homeland Security Workload

Both DHS and DTC have existing informal relationships in a few specialized areas. If DTC and DHS S&T formalize this relationship and a large shift of workload is added to the test centers, a portion of the DTC workforce and facilities would be dedicated to that support. A certain level of work throughput also would be required to sustain this effort.

If DHS S&T decides to build its own facilities or sever the existing relationship, DTC will be required to account for this workload void. This can be done through seeking new customers, downsizing the workforce, or closing facilities primarily used by DHS S&T. This would require significant administrative effort.

Changes in U.S. Department of Homeland Security Science and Technology Needs

The technology needs identified by DHS S&T are in constant flux. The technology needs are very susceptible to the external environment and may have to change. The change in threats may require testing facilities and infrastructure not available to DTC. Additionally, testing needs that were once relevant can suddenly become obsolete. DTC would be required to be extremely flexible.

This uncertainty could make planning difficult. If the technology development needs are constantly changing, so are the test needs. Planning for future workload by DTC to support DHS S&T could be next to impossible. This problem is compounded by the different funding mechanisms that DHS S&T uses to support DTC test services.

Outside of Primary Mission

As a U.S. Army asset, DTC is required to fulfill the needs of the U.S Army before it meets the needs of its external customers. From the perspective of stakeholders, it can be easy not to understand why a DoD asset is being used for a DHS requirement. Unfortunately, DHS S&T technology programs can experience lower prioritization of their tests. This can lead to delays in schedule and costs to DHS S&T. Historically, loss of prioritization results in customers who are dissatisfied with the DTC testing experience, which can impact the organization's credibility.

CHAPTER 5

CONCLUSIONS AND RECOMMENDATIONS

Conclusions

The data in this research paper confirms the hypothesis that the U.S. Federal Government would benefit from a partnership between the DHS S&T and DTC. The level of benefit that the U.S. Federal Government would receive was not fully demonstrated.

In proving the hypotheses, this research paper validated Critical Assumption 1: Not all potential relationships between the DTC test infrastructure and the DHS S&T test requirements have been fully exploited. Using the matrix design to compete a crosswalk between the technology needs of DHS S&T and the testing capabilities of DTC, the data demonstrate numerous areas can be exploited beyond what has been completed historically.

In addition, this paper partially validates Critical Assumption 2: The DHS S&T test infrastructure needs are very similar to the existing DTC testing capabilities. The matrix design shows that the technology test needs of DHS S&T are very similar to the existing capabilities of DTC in some but not all of the Capstone IPT technology areas.

The Capstone IPTs that show significant matches with the DHS capability areas include border security, cargo security, counter IED, and transportation security. Although the chemical and biological defense capstone IPT is classified as a partial match, the program is of large significance and there are a limited number of facilities capable of conducting this type of testing. Therefore, a partnership should be evaluated.

The data also demonstrates capability gaps remain between the two organizations after the crosswalk. DHS S&T will be required to use other providers of test infrastructure to meet needs of the Capstone IPTs' areas of cyber-security, incident management, and information sharing.

The SWOT analysis demonstrates that establishing a partnership between DHS S&T and DTC would not be a simple task. Although it is clear that the strengths and weaknesses complement each other and the opportunities are abundant, numerous external factors would threaten this partnership. This paper shows that a partnership is possible but must be further evaluated on a tactical level.

Recommendations

The fidelity of the SWOT analysis in this plan does not allow for the detail required to give specific recommendations on the best method to partner in the future. A follow-up implementation plan should be developed to identify each organization's interests, expectations, and requirements (IER). Based on this IER, representatives from each organization would determine the best method to partner. The action plan would serve as a strategic communication tool. Implementation of the action plan will require the participation and input from all levels of the both organizations' workforces. The leadership could use the action plan as a mechanism to describe the reasoning, mechanisms, vision, and steps required to make the effort successful.

Representatives from DTC should seek the leaders of the Capstone IPTs that have significant matches between the organizations. There should be critical dialogues to determine appropriate level of support and synergy. This will allow the DHS S&T leadership to fully understand DTC capabilities, facilities, and opportunities.

A memorandum of agreement between DTC and DHS S&T should be developed to allow an easy interagency transfer of resources to support developmental testing in the DTC core competency areas. During development of this agreement, the multiple opportunities and threats identified in the research should be addressed. In addition, it would establish clear processes that DHS S&T and DTC can use to guide their partnership.

A major limitation of this research paper is that it focuses only on developmental testing. As mentioned earlier, effective test and evaluation strategy requires both developmental and operational testing. Additional research is recommended to expand the matrix design crosswalk and include operational test capabilities of OTC.

In the midst of the work on this research paper, a major reorganization of ATEC was announced in conjunction with the relocation of the headquarters from Alexandria, VA, to APG, MD. At the time of publishing, the final organizational structure, mission, vision, and strategy were not formalized. There is a significant possibility that DTC will be dramatically changed by the middle of 2011. If this is the case, the findings here are still valid toward whichever organization retains responsibility for the developmental test mission of the U.S. Army.

PAGE LEFT BLANK INTENTIONALLY

REFERENCES

Buswell, B. (2009). "U.S. Department of Homeland Security, Science and Technology, High-Priority Technology Needs" (Version 3.0). U.S. Department of Homeland Security, Washington, DC.

Carafano, J. Czerwinski, J., &Weitz, R. (2006). "Homeland Security Technology, Global Partnerships, and Winning the Long War." The Backgrounder, 1977.

Cast, M. (2010). "New Director Assumes Responsibility for Army Developmental Test Ccommand." U.S. Army Developmental Test Command Press Release.

Cellucci, T. (2010). "Research & Development Partnerships Group: Working With You to Serve the Homeland Security Enterprise." U.S. Department of Homeland Security, Washington, DC.

Chertoff, M. (2008). "U.S. Department of Homeland Security – One Team, One Mission, Securing Our Homeland," (U.S. Department of Homeland Security Strategic Plan Fiscal Years 2008-2013). U.S. Department of Homeland Security, Washington, DC.

Cohen, J. (2007). "U.S. Department of Homeland Security: Science and Technology Strategy to Make a Nation Safer." U.S. Department of Homeland Security, Washington, DC.

Coman, A., & Ronen, B. (2009). "Focused SWOT: Diagnosing Critical Strengths and Weaknesses." International Journal of Production Research, 47 (20), 5677-5689.

Coursey, B. (2008). "DHS S&T standards, building confidence in homeland security technologies." U.S. Department of Homeland Security, Washington, DC.

Duke, E. (2010). U.S. Department of Homeland Security directives (System Directive No. 102-01, Subject: Acquisition Management Directive). Washington, DC.

England, G. (2007). U.S. Department of Defense directive (No. 3200.11, Subject: Major Range and Facility Test Base.) Washington, DC.

Everett, R., & Duval, C. (2010). "Some Considerations for the Use of Strategic Planning Models." Proceedings for the Northeast Region Decision Sciences Institute (NEDSI), 525-530.

International Test and Evaluation Association. (2007). George Washington Chapter Newsletter, *17 (9)*.

Hale, J. (2005). U.S. Department of Homeland Security directives (System Directive No. 0784, Subject: Acquisition Oversight Program). Washington, DC.

Hite, R. C. (2010). "Secure Border Initiative: Testing and Problem Resolution Challenges Put Delivery of Technology Program At Risk" (Congressional Testimony). Washington, DC.

Levesque, J., & Walker, F. (2007). "The Innovation Process and Quality Tools." Quality Progress, 40 (7),18-22.

Maze, R. (2011). "Money DoD Saves May Be Cut From Budget." Air Force Times.

Orszag, P. (2009). Open-Government Directive (Directive, M-10-06). Office of Management and Budget, Washington, DC.

Ryynänen, T., & Jansson, K. (2007). "A Method to Advance Mutual Understanding In a Multi-Partnership Project." The Business Review, 8 (1), 326-331.

Sluismans, R., Lommelen, T., & den Hertog, F. (2010). "The use of SWOT as a tool to stimulate strategic conversation in SMEs." IIE Annual Conference Proceedings.

Tague, N. (2005) The Quality Toolbox: Second Edition. ASQ Quality Press, Milwaukee, WI.

Undersecretary of Defense for Acquisition, Logistics, and Technology (2008). Report of the Defense Science Board Task Force on Developmental Testing. Washington, DC.

U.S. Department of the Army. (2006). Development Test Policy (Developmental Test Command Regulation 73-1). Headquarters, U.S. Army Developmental Test Command. Aberdeen Proving Ground, MD.

U.S. Department of the Army. (2009a). "Mission and Major Capabilities of the U.S. Army Aberdeen Test Center" (Developmental Test Command Regulation 10-3). Headquarters, U.S. Army Developmental Test Command, Aberdeen Proving Ground, MD.

U.S. Department of the Army. (2009b). "Mission and Major Capabilities of the U.S. Army Dugway Proving Ground" (Developmental Test Command Regulation 10-7). Headquarters, U.S. Army Developmental Test Command, Aberdeen Proving Ground, MD.

U.S. Department of the Army. (2009c). "Mission and Major Capabilities of the U.S. Army Electronic Proving Ground" (Developmental Test Command Regulation 10-9). Headquarters, U.S. Army Developmental Test Command, Aberdeen Proving Ground, MD.

U.S. Department of the Army. (2009d). "Mission and Major Capabilities of the U.S Army Redstone Test Center" (Developmental Test Command Regulation 10-4). Headquarters, U.S. Army Developmental Test Command, Aberdeen Proving Ground, MD.

U.S. Department of the Army. (2009e). "Mission and Major Capabilities of the U.S. Army White Sands Missile Range" (Developmental Test Command Regulation 10-6). Headquarters, U.S Army Developmental Test Command, Aberdeen Proving Ground, MD.

U.S. Department of the Army. (2009f). "Mission and Major Capabilities of the U.S. Army Yuma Proving Ground" (Developmental Test Command Regulation 10-5). Headquarters, U.S. Army Developmental Test Command, Aberdeen Proving Ground, MD.

U.S. Department of Homeland Security. (2008a). "Brief Documentary History of the Department of Homeland Security" (2001-2008). Washington, DC.

U.S. Department of Homeland Security. (2008b). "Science and Technology for a Safer Nation." Washington, DC.

U.S. Department of Homeland Security. (2008c). "Top Ten Challenges Facing the Next Secretary of Homeland Security." Washington, DC.

U.S. Government Accountability Office. (2004). "U.S. Department of Homeland Security: DHS Needs a Strategy to Use DOE's Laboratories for Research on Nuclear, Biological, and Chemical Detection and Response Technologies" (GAO-04-653). Washington, DC.

U.S. Government Accountability Office. (2007a). "U.S. Department of Homeland Security: Ongoing Challenges in Creating an Effective Acquisition Organization" (GAO-07-948T). Washington, DC.

U.S. Government Accountability Office. (2007b). "U.S. Department of Homeland Security: Assessments of Selected Complex Acquisitions" (GAO-10-588SP). Washington, DC.

U.S. Government Accountability Office. (2009). U.S. Department of Homeland Security: A Strategic Approach is Needed to Better Ensure the Acquisition Workforce Can Meet Mission Needs" (GAO-09-30). Washington, DC.

LIST OF ACRONYMS

AEC – U.S. Army Evaluation Center

APG – Aberdeen Proving Ground

ATEC – U.S. Army Test and Evaluation Command

CBRNE – Chemical, Biological, Radiological, Nuclear, and Explosive

DoD – U.S. Department of Defense

DOE – U.S .Department of Energy

DHS – U.S. Department of Homeland Security

DHS S&T – U.S. Department of Homeland Security Science and Technology Directorate

DTC – U.S .Army Developmental Test Command

GAO – U.S. Government Accountability Office

IED – Improvised Explosive Device

IER – Interests, Expectations, and Requirements

IPT – Integrated Product Team

MRTFB – Major Range Test Facility Base

OMB – Office of Management and Budget

OTC – U.S. Army Operational Test Command

R&D – Research and Development

SWOT – Strengths, Weaknesses, Opportunities, and Threats

TSWG – Technical Support Working Group

PAGE LEFT BLANK INTENTIONALLY

APPENDIX A:

DHS S&T NEEDS VS. DTC CAPABILITIES CHART

	Active Protection Systems	Air Delivery Systems/Air Drop	Air/Missile Defense Systems	Aircraft Systems	Antenna Testing	Army Test Incident Reporting System	Automotive Vehicles	Chemical and Biological Defense	Command, Control, Communications, and Computers	Counter-Terrorism/Counter Insurgency	Directed Energy Weapons	Direct Fire Systems	Electromagnetic Environmental Effects	Electronic Countermeasures - IED	Electronic Warfare	Emissions characterization - Air	Engineering Equipment	Environmental Mitigation Technologies	Extreme Natural Environments	Force Protection Systems	Foreign Weapons Systems	Homeland Defense Technologies - Explosive Detection	Human Factors Engineering/MANPRINT	Indirect Fire Systems	Intelligence, Surveillance, and Reconnaissance	Littoral Warfare	Meteorological Technology Development	MIL-STD-810 Environmental Testing	Missiles/Rockets	Non-lethal Weapons	Nuclear Weapons Effects	Optical and Electro-optical systems	Reliability, Availability, Maintainability	Smoke and Obscurants	SOMARDS Financial Information Management System	Soldier Systems	Systems of Systems Integration	System Safety	Telecommunications Emission Security	Transportability	Unmanned Aircraft Systems	Unmanned Ground Vehicles	Vulnerability/Lethality	
Border Security IPT																																											
Detect, track, and classify border threats										x															x																		
Inspection of closed compartments										x												x													x							
Non-lethal compliance of orders							x														x								x					x							x
Analysis and decision making tools																																											
Non-lethal interdiction compliance				x							x			x						x						x			x												x
Cargo Security IPT																																											
Non intrusive inspection for contraband																						x													x							
Automated target recognition																						x																				
Screening of air cargo (100%)																						x																				
Track domestic high-threat cargo																																										
Cargo intrusion detection																						x																				
Container inspection for hazard materials								x														x																				
Chemical/Biological Defense IPT																																											
Chem/bio forensic analysis								x																																			
Handheld rapid chem/bio detection								x																											x								
Paradigms for new bio threats																																											
Tools for animal disease																																											
Data fusion for bio surveillance																																											
National chem/bio detection architecture																																											
Tools for consequence analysis on chem/bio attack																																											
Common operating picture for sensors								x																											x								
New chemical analysis techniques								x																																			
Risk assessment tools																																											
Incident characterization																																											
Chem/bio detection in buildings								x																																			
Validation of commercial assays								x																											x								
Decontamination of infrastructure																																											
Inspection of packages for chem/bio								x																																			

	Active Protection Systems	Air Delivery Systems/Air Drop	Air/Missile Defense Systems	Aircraft Systems	Antenna Testing	Army Test Incident Reporting System	Automotive Vehicles	Chemical and Biological Defense	Command, Control, Communications, and Computers	Counter-Terrorism/Counter Insurgency	Directed Energy Weapons	Direct Fire Systems	Electromagnetic Environmental Effects	Electronic Countermeasures - IED	Electronic Warfare	Emissions characterization - Air	Engineering Equipment	Environmental Mitigation Technologies	Extreme Natural Environments	Force Protection Systems	Foreign Weapons Systems	Homeland Defense Technologies - Explosive Detection	Human Factors Engineering/MANPRINT	Indirect Fire Systems	Intelligence, Surveillance, and Reconnaissance	Littoral Warfare	Meteorological Technology Development	MIL-STD-810 Environmental Testing	Missiles/Rockets	Non-lethal Weapons	Nuclear Weapons Effects	Optical and Electro-optical systems	Reliability, Availability, Maintainability	Smoke and Obscurants	SOMARDS Financial Information Management System	Soldier Systems	Systems of Systems Integration	System Safety	Telecommunications Emission Security	Transportability	Unmanned Aircraft Systems	Unmanned Ground Vehicles	Vulnerability/Lethality
Counter IED IPT																																										
Novel computational models																																										
Predictive behavioral models																																										
Detection of vehicle borne IED							x			x				x							x	x																				
Detection of person borne IED										x				x							x	x																				
Defeat of vehicle borne IED							x			x	x			x	x						x																				x
Defeat of person borne IED										x	x			x	x						x																				x
Diagnose vehicle or personnel borne IED							x			x												x																			
Diagnose and defeat water borne IED										x												x				x															x
Characterize IEDs										x																															x
Cyber Security IPT																																									
Secure internet protocols																																									
Modeling cyber attacks																																									
Software testing									x						x																										
Usable security																																									
Insider threat detection																																									
IT system engineering security									x						x																										
Process control systems																																									
Cyber forensics																																									
First Responder IPT																																									
Defeat explosives										x				x								x																		x	x
Non-lethal compliance (people, vehicles, vessels, aircraft)				x			x			x																x				x					x						
Inspection of closed compartments										x												x													x						
Chemical detection								x		x												x																			
Disaster preparedness																																									
Respiratory protection (PM, gas, chemical, biological)								x																									x		x		x					
Predicting criminal/terrorist activity																																									
First responder training																																									
Ambulance command and control									x																																
Credential verification																																									
Emergency manager command and control									x																																
Information management																																									

	Active Protection Systems	Air Delivery Systems/Air Drop	Air/Missile Defense Systems	Aircraft Systems	Antenna Testing	Army Test Incident Reporting System	Automotive Vehicles	Chemical and Biological Defense	Command, Control, Communications, and Computers	Counter-Terrorism/Counter Insurgency	Directed Energy Weapons	Direct Fire Systems	Electromagnetic Environmental Effects	Electronic Countermeasures - IED	Electronic Warfare	Emissions characterization - Air	Engineering Equipment	Environmental Mitigation Technologies	Extreme Natural Environments	Force Protection Systems	Foreign Weapons Systems	Homeland Defense Technologies - Explosive Detection	Human Factors Engineering/MANPRINT	Indirect Fire Systems	Intelligence, Surveillance, and Reconnaissance	Littoral Warfare	Meteorological Technology Development	MIL-STD-810 Environmental Testing	Missiles/Rockets	Non-lethal Weapons	Nuclear Weapons Effects	Optical and Electro-optical systems	Reliability, Availability, Maintainability	Smoke and Obscurants	SOMARDS Financial Information Management System	Soldier Systems	Systems of Systems Integration	System Safety	Telecommunications Emission Security	Transportability	Unmanned Aircraft Systems	Unmanned Ground Vehicles	Vulnerability/Lethality
Incident Management IPT																																										
Simulation based training system																																										
Personnel monitoring (location)									x														x											x		x						
Personnel monitoring (physiological)																							x													x						
Incident management enterprise system																																										
Logistics management tool																																										
Information Sharing IPT																																										
User-Defined operating picture																																										
User management																																										
Classified information distribution																																										
Cross sectional threat sharing																																										
Increased situational awareness																																										
Predictive analytics																																										
Protection of personally identifiable information																																										
Reporting of suspicious activity																																										
Infrastructure Protection IPT																																										
Tools for infrastructure interdependencies																																										
Explosive blast analysis and protection																																										x
Decision support systems																																										
Rapid mitigation and recovery technologies																																										
Transportable critical utility components																																x		x				x				
Early warning system for levee failure																																										
Interoperability IPT																																										
Standards for voice over internet protocol																																										
Wireless broadband technologies																																										
Message interface standards																																										
Testing of emergency response devices									x						x																							x				
Multi-band radio technologies									x						x																							x				
Single unified communication device																																										
Ad-hoc and mesh networks																																										

	Active Protection Systems	Air Delivery Systems/Air Drop	Air/Missile Defense Systems	Aircraft Systems	Antenna Testing	Army Test Incident Reporting System	Automotive Vehicles	Chemical and Biological Defense	Command, Control, Communications, and Computers	Counter-Terrorism/Counter Insurgency	Directed Energy Weapons	Direct Fire Systems	Electromagnetic Environmental Effects	Electronic Countermeasures - IED	Electronic Warfare	Emissions characterization - Air	Engineering Equipment	Environmental Mitigation Technologies	Extreme Natural Environments	Force Protection Systems	Foreign Weapons Systems	Homeland Defense Technologies - Explosive Detection	Human Factors Engineering/MANPRINT	Indirect Fire Systems	Intelligence, Surveillance, and Reconnaissance	Littoral Warfare	Meteorological Technology Development	MIL-STD-810 Environmental Testing	Missiles/Rockets	Non-lethal Weapons	Nuclear Weapons Effects	Optical and Electro-optical systems	Reliability, Availability, Maintainability	Smoke and Obscurants	SOMARDS Financial Information Management System	Soldier Systems	Systems of Systems Integration	System Safety	Telecommunications Emission Security	Transportability	Unmanned Aircraft Systems	Unmanned Ground Vehicles	Vulnerability/Lethality
Maritime Security IPT																																										
Wide area surveillance																									x	x																
Track contraband on ships										x																x															
Non-lethal compliance (vessels)										x																x			x												
Chemical detection								x		x																x															
Radar tracking of vessels																									x	x															
People Screening IPT																																										
Data fusion and M&S for terrorist intent																																										
Non-invasive behavior sensors																																										
Identification through biometrics																																										
Mobile biometric devices										x																									x						
High speed fingerprinting										x																									x						
Rapid DNA testing																																										
Biometric detection at distance										x																									x						
Advanced imaging at checkpoints										x																				x					x						
Transportation Security IPT																																										
Screening people for explosives & weapons																						x																			
Screening cargo for explosives																						x																			
Automated system for explosive detection																						x																			
Canine explosive detection																						x																			
Detection of homemade explosives																						x																			

PAGE LEFT BLANK INTENTIONALLY

APPENDIX B:

STRENGTHS, WEAKNESSES, OPPORTUNITIES, AND THREATS ANALYSIS CHARTS

Strengths

- DHS technologies are typically commercial off-the-shelf and are tied to known standards.
- DHS has existing testing partnerships.
- DHS displays organizational flexibility.
- DHS leadership supports partnering and coordination.

Weaknesses

- DHS acquisition workforce is not fully staffed, experienced, or trained
- DHS acquisition program is immature and unstable
- DHS has limited internal test infrastructure
- DHS has no organization coordinating test and evaluation results or execution

Opportunities

- DHS does not have to develop acquisition system or workforce from scratch.
- DHS can leverage government partnerships for joint technology development and testing.
- DHS can remove appearance of conflict of interest while using experience of DTC.
- DHS entering formal relationship can produce efficiency, priority, and reciprocity.

Threats

- DHS operates under a great deal of congressional oversight.
- DHS acquisition programs funding is based on the national economy.
- DHS' existing relationships could be threatened since this would be seen as draining resources from R&D and national labs.
- DHS and Army culture may not be compatible

Strengths

- DTC existing test facilities, capabilities, and infrastructure
- DTC mature and experienced acquisition workforce
- DTC linkage to the Army evaluation community
- DTC credibility in the test and evaluation community

Weaknesses

- DTC current informal and disjointed relationship with DHS S&T
- DTC lack of operational testing responsibility
- DTC existing workload
- DTC financial stability

Opportunities

- DTC gains political capital and increases stature
- DTC workload diversity increased
- DTC and DHS S&T leverage expertise and capabilities
- DTC gains partner to resource dual-use test infrastructure

Threats

- DTC impacted by DOD efficiency efforts
- DTC reliance on DHS S&T to sustain workload and infrastructure
- DTC ability to meet DHS S&T changing testing needs and threats
- Changes in political and military leadership impacting relationships
- Outside of DTC's primary mission